REMARKS

The Office Action dated December 5, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 18, 42, 55, 59, 63, 64 and 66-68 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 5 has been canceled without prejudice or disclaimer. No new matter has been added and no new issues are raised which require further consideration or search.

The Office Action objected to the IDS for failing to include the proper page designations required under 37 CFR 1.97. Applicants have submitted a new IDS that includes page numbers which accurately identify the total pages included in each of the cited documents. Accordingly, consideration of each of the references cited on the IDS is respectfully requested.

The Office Action rejected claims 66-68 under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter. The Office Action alleged that the claims may be considered software *per se* and since they are not embodied on a computer readable storage medium. Applicants have amended claims 66-68 to recite a "computer readable storage medium." Accordingly, Applicants submit that the claims are in compliance with 35 U.S.C. §101. Withdrawal of the rejection is kindly requested.

Claims 1, 2, 5-10, 15, 18-20, 42, 43, 45-49, 55, 56, 58-60 and 62-65 were rejected under 35 U.S.C. §102(b) as being anticipated by Gupta et al. (U.S. Patent No. 6,389,532). Applicants respectfully traverse this rejection.

Claim 1, upon which claims 2, and 4-15 are dependent, recites a method that includes generating validity information for a packet. The validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and no pre-established security association is needed to verify the packet. The method further provides generating a packet header including the validity information, and including generating the algorithm information which includes values to initialize an algorithm to be used to perform the validity check of the packet. The method also includes sending the packet including the header from a first network node to a second network node.

Claim 18 recites an apparatus that includes validity information generating means for generating validity information for a packet. The apparatus also includes packet header generating means for generating a header for the packet, comprising the validity information, and sending means for sending the packet including the header to a receiving network node. The apparatus further provides that the validity information includes all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of

the packet. The algorithm information includes values to initialize an algorithm to be used to perform the validity check of the packet.

Claim 42, upon which claims 43-54 are dependent, recites an apparatus that includes a validity information generator configured to generate validity information for a packet. The apparatus also includes a packet header generator configured to generate a header for the packet that includes the validity information. The apparatus also includes a transmitter configured to send the packet including the header to a receiving network node. The validity information includes all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet. The algorithm information includes values to initialize an algorithm to be used to perform the validity check of the packet

Claim 55, upon which claims 56-58 are dependent, recites an apparatus that includes a receiver configured to receive packets from a sending network node. The apparatus includes a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet. The validity information includes all necessary information required to perform the validity check of the packet and no pre-established security association is needed to verify the packet. The validity information includes algorithm information to be used to perform the validity check of the packet. The algorithm information includes values to initialize an algorithm to be used to perform the validity check of the packet

Claim 59, upon which claims 60-62 are dependent, recites an apparatus that includes a transmitter configured to forward packets from a sending network node to a receiving network node. The apparatus also includes a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet. The validity information includes all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet. The validity information includes algorithm information to be used to perform the validity check of the packet. The algorithm information includes values to initialize an algorithm to be used to perform the validity check of the packet

Claim 63 recites a method that includes receiving packets, and performing a validity check of a packet by referring to validity information contained in a header of the packet. The validity information includes all necessary information required to perform the validity check of the packet and no pre-established security association is needed to verify the packet. The validity information includes algorithm information to be used for performing the validity check of the packet.

Claim 64 recites a method that includes forwarding received packets, and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet. The validity information includes all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information includes algorithm information to be used for performing the validity check of the packet.

The algorithm information includes values to initialize an algorithm to be used to perform the validity check of the packet.

Claims 66-68 are computer program-type variations of at least one or more of the above claims. However, claims 66-68 each has its own scope and should be interpreted as such.

As will be discussed below, the teachings of Gupta fail to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above. The rejection is respectfully traversed for at least the following reasons.

Gupta discloses filtering packets in a network using digital signatures. A router or firewall is used to test the validity of the digital signature using a public key (see Abstract of Gupta). Based on the validity of the signature, the packet is either discarded or forwarded (see Fig. 7 of Gupta). Referring to Fig. 3 of Gupta, the structure of a packet includes a packet header 302 which comprises a fingerprint 308, a signature 310, a key index 312 and IP header options 322.

In Gupta, a query is performed on a DNS server in order for the owner to obtain validity keys (see column 6, lines 7 and 8 of Gupta). Gupta further discloses that the owner 106 distributes these private keys to authorized senders in operation 508 of FIG. 5. (see column 6, lines 16-18 of Gupta). According to Gupta a receiver (owner 106) and a sender (authorized sender) must communicate with a third entity (DNS server 412) in order to confirm the validity of the information.

On column 3, lines 41-48 of Gupta, a process describes how the packet is generated. In particular, a fingerprint corresponding to data contained in the packet is generated, and the fingerprint is encrypted using the sender's private key. The encrypted fingerprint is used as the signature. This is also evident from Fig. 6 and column 6, lines 25-55 of Gupta. According to Gupta the algorithm used to handle the packet fingerprint must be known beforehand. Step 602 of Fig. 6 clearly illustrates that the necessary private keys are exchanged before the packet is transmitted.

Gupta is directed to the same disadvantages described on page 2 of the introduction of the present application, as noted above. Gupta does not describe generating a packet header with validity information to be used to perform the validity check of the packet. It is clear from Fig. 6 and column 6, lines 25-55 of Gupta that all of the validity information generated for a packet is not in a packet header of the packet, as recited in claim 1.

Gupta is directed to the type of prior art recognized by the patent application and does not disclose the subject matter recited in independent claim 1 and similarly recited in independent claims 18, 42, 55, 59, 63, 64 and 66-68. For instance, independent claim 1 recites "generating validity information for a packet...the validity information comprising algorithm information...generating a packet header, comprising the validity information, and comprising generating the algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet." It is clear from the claim recitations of claim 1, that the validity information generated

includes the algorithm information and that each of these pieces of information are part of the packet header. As a result of providing the algorithm information and values to initialize the algorithm in the packet header, the reliability of the packets may be checked without the need for a pre-established security association.

The Office Action relied on FIG. 7 which is described at column 7, lines 12 to 19 of Gupta as allegedly disclosing a validity information that requires all necessary information to perform a validity check of the packet and that no pre-established security association is needed to verify the packet (see page 7, lines 9-12 of the Office Action). However, applicants submit that Gupta discloses details of the operations of FIG. 7 that are contrary to the Office Action's interpretations. For instance, referring to column 7, lines 5 to 10, it is clearly disclosed that the router 104 determines whether a signature is required by checking a flag 213 in storage 204. That is, before obtaining a public key or performing a similar operation, the router first checks whether a signature is required. In such a case, the router 104 discards the packet at step 710 if no signature is present.

The router checks the packet by referring to the flag, which is stored in the router's own storage. Only when the flag is set to particular predefined value, then the router checks whether it has the public key available or whether it has to obtain it from a DNS (see column 7, lines 10-16 of Gupta). The flag is stored in the router's storage and thus must be set prior to being checked. The packet itself has no packet header that includes "validity information" and "algorithm information which comprises values to initialize an

algorithm to be used to perform the validity check of the packet", as recited in independent claim 1.

As for column 6, lines 25 to 32 of Gupta,it is disclosed that the sender obtains a private key and key index separately at some time before actually sending packets. Applicants submit that this process relates to the sender and not the receiver. Regardless of the origin of the key obtaining process, there is some kind of security association that is established beforehand and which stems beyond the security provided by information provided in a packet header.

Applicants have cancelled claim 5 and have incorporated its subject matter into each of the independent claims 1, 18, 42, 55, 59, 63, 64 and 66-68. Furthermore, with respect to the rejection of claim 5, the Office Action referred to column 6, paragraphs 3 to 4 of Gupta as allegedly providing support for claim 5. Referring to column 6 of Gupta, it appears that there is some information (i.e,. a signed fingerprint) which might be included in the packet and later verified during a packet verification process. However, this information is not used to initialize any algorithm, and, certainly does not include "algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet", as recited in independent claim 1.

As stated in claim 1, the validity information comprises all necessary information required to perform a validity check of the packet, and, in particular, comprises algorithm information with respect to the algorithm used to perform the validity check of the packets and the information necessary to initialize the algorithm. The validity checks can

be handled flexibly in the network, since each network node involved in the packet communication can obtain the required algorithm information as needed for verification. Contrary to the subject matter recited in claim 1 of the present application, Gupta discloses a method and apparatus for filtering packets that does not include the same packet verification features recited in claim 1.

Therefore, for at least the reasons stated above, Applicants submit that Gupta fails to teach all of the subject matter recited in independent claims 18, 42, 55, 59, 63, 64 and 66-68. By virtue of dependency claims 2, 4-15, 43-54, 56-58 and 60-62 are also allowable over Gupta. Withdrawal of the rejection of claims 1, 2, 5-10, 15, 18-20, 42, 43, 45-49, 55, 56, 58-60 and 62-65 is respectfully requested.

Claims 4, 12-14, 44, 51-53, 57 and 61 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Gupta in view of Naudus (U.S. Patent No. 6,202,081). This rejection is respectfully traversed.

Gupta is discussed above. Naudus discloses a method and protocol for synchronized transfer-window based firewall traversal. In column 6, line 60, to column 7, line 7 of Naudus, a security association is described which may also indicate an encryption technique (i.e., the hashed message authentication code (HMAC) keyed-message digest-5 (MD5)). A security association, however, requires establishing the security association, and the exchange of several messages beforehand prior to a packet transmission. Therefore, Naudus shares the same disadvantages as Gupta which is directed to the prior art described in the present application.

Claims 4, 12-14, 44, 51-53, 57 and 61 are dependent upon claims 1, 18, 42, 55 and 59 and contain all of the limitations thereof. As discussed above, the teachings of Gupta fails to disclose or suggest all of the elements of claims 1, 18, 42, 55 and 59. In addition, Naudus fails to cure the deficiencies in Gupta as Naudus also fails to disclose or suggest "generating validity information for a packet...the validity information comprising algorithm information...generating a packet header, comprising the validity information, and comprising generating the algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet" as recited in claim 1 and similarly in claims 1, 18, 42, 55 and 59. Accordingly, the combination of Gupta and Naudus fails to disclose or suggest all of the elements of claims 4, 12-14, 44, 51-53, 57 and 61. Furthermore, claims 4, 12-14, 44, 51-53, 57 and 61 should be allowed for at least their dependence upon claims 1, 18, 42, 55 and 59, and for the specific limitations recited therein.

Claims 11 and 50 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Gupta in view of Nikander (U.S. Patent No. 7,155,500). This rejection is respectfully traversed.

Gupta is discussed above. Nikander discloses a method of verifying that a host coupled to an IP network is authorized to use an IP address. The IP address comprising a routing prefix and an interface identifier part. The method comprises receiving from the host one or more components, applying a one-way coding function to the or each component and/or derivatives of the or each component, and comparing the result or a

derivative of the result against the interface identifier part of the IP address. If the result or its derivative matches the interface identifier the host is assumed to be authorized to use the IP address and if the result or its derivative does not match the interface identifier the host is assumed not to be authorized to use the IP address.

Claims 11 and 50 are dependent upon claims 1 and 42 and contain all of the limitations thereof. As discussed above, the teachings of Gupta fails to disclose or suggest all of the elements of claims 11 and 50. In addition, Nikander fails to cure the deficiencies in Gupta as Nikander also fails to disclose or suggest "generating validity information for a packet...the validity information comprising algorithm information...generating a packet header, comprising the validity information, and comprising generating the algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet" as recited in claim 1 and similarly in claim 42. Accordingly, the combination of Gupta and Nikander fails to disclose or suggest all of the elements of claims 11 and 50. Furthermore, claims 11 and 50 should be allowed for at least their dependence upon claims 1 and 42, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-2, 4-15, 18-20 and 42-65 be allowed, and this application passed to issue.

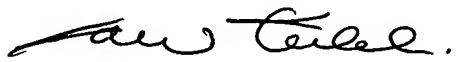
The Nauda reference was cited in the present Office Action, however, neither for the independent claims nor for claim 5 now included into claim 1. It is, however, believed that the arguments with respect to Nauda are still correct. Hence, please refer to the earlier comments and replies.

For at least the reasons discussed above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims ggg be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Kamran Emdadi
Registration No. 58,823

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

KE:sjm

Enclosures: Petition for Extension of Time
Check No. 20603
Information Disclosure Statement